#4

Attorney Docket No. 1454.1212

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Christian ENSEL et al.

Application No.: 10/042,278 Group Art Unit: 2152

Filed: January 11, 2002 Examiner:

For: SYSTEM FOR MONITORING TELECOMMUNICATION NETWORK AND TRAINING STATISTICAL ESTIMATOR

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

German Patent Application No. 101 01 286.1

Filed: 12 January 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3/27/02

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 31,106

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 01 286.1

Anmeldetag: 12. Januar 2001

Anmelder/Inhaber: Siemens Aktiengesellschaft, München/DE

Bezeichnung: Verfahren und Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes, Verfahren zum rechnergestützten Trainieren eines statistischen Schätzers, Computerlesbare Speichermedien und Computerprogramm-Elemente

IPC: H 04 L 12/26

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 4. Januar 2002
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Joost

A 9161
06/00
EDV-L

Beschreibung

Verfahren und Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes, Verfahren zum rechnergestützten Trainieren eines statistischen Schätzers, Computerlesbare Speichermedien und Computerprogramm-Elemente

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes sowie ein Verfahren zum rechnergestützten Trainieren eines statistischen Schätzers zum Überwachen eines Telekommunikationsnetzes.

In einem üblichen Telekommunikationsnetz, beispielsweise dem Internet, sind eine Vielzahl sehr unterschiedlicher kommunikationsfähiger Geräte miteinander vernetzt, das heißt gekoppelt.

Unter einem Telekommunikationsnetz ist in diesem Zusammenhang ein Kommunikationsnetz zu verstehen, mittels dem unterschiedliche elektronische Geräte miteinander kommunizieren können, beispielsweise

- ein Kommunikationsnetz, welches eine Kommunikation gemäß den Internet-Protokollen ermöglicht,
- ein lokales Kommunikationsnetz (Local Area Network, LAN),
- ein öffentliches Kommunikationsnetz, welches auch als Wide Area Network (WAN) bezeichnet wird,
- ein Funknetz, beispielsweise gemäß dem GSM-Standard oder dem UMTS-Standard.

In einem solchen inhomogenen Kommunikationsnetz, das heißt in einem Kommunikationsnetz mit sehr vielen unterschiedlichen elektronischen Geräten, die nicht auf dem gleichen Betriebssystem, Kommunikationsmechanismus, etc., basieren, besteht oftmals das Erfordernis, diese Geräte gemeinsam zu verwalten und/oder zu überwachen, beispielsweise hinsichtlich eines

Ausfalls eines der in dem Kommunikationsnetz miteinander gekoppelten Geräten oder hinsichtlich unterschiedlicher Eindringversuche oder Angriffsversuche, die ein unbefugtes Eindringen in die gespeicherten Daten eines solchen Geräts darstellen.

Durch die Vielzahl an unterschiedlichen Arten von mit dem Kommunikationsnetz miteinander gekoppelten Geräten, beispielsweise

- Vermittlungseinheiten,
- kommunikationsfähige Endgeräte wie
  - Drucker,
  - Server-Computer,
  - Workstations,
  - Personal Computer,
  - Laptops,
  - Personal Digital Assistants (PDAs), etc.

und aufgrund der Komplexität der unterschiedlichen Arten der Kommunikationsverbindungen zwischen den einzelnen Geräten, die auf unterschiedlichen Kommunikationsstandards, d.h. Kommunikationsprotokollen, basieren können, sind derzeit Geräte in einem Telekommunikationsnetz nur in sehr beschränktem Ausmaß automatisiert zentral zu verwalten und zu überwachen.

Weiterhin besteht oftmals das Erfordernis, nicht nur die Geräte selbst, sondern auch Dienste, das heißt im Sinne der weiteren Beschreibung beispielsweise Anwendungsprogramme in Ausführung, wie ein Webserver, ein Dateiserver, Datenbanken, verschiedene Anwendungsserver oder X11-Terminals, die ebenfalls miteinander über das Telekommunikationsnetz kommunizieren, zu verwalten und/oder zu überwachen.

Aufgrund einer derzeit mangelhaften automatisierten zentralen Überwachungsmöglichkeit ist es nur schwer, wenn überhaupt, möglich, einen Ausfall oder einen Angriffsversuch auf ein Gerät und/oder einen Dienst zu erkennen und rechtzeitig auf einen solchen Ausfall bzw. Angriffsversuch zu reagieren.

Weiterhin wird oftmals durch einen Ausfall oder einen Angriffsversuch eines Geräts bzw. eines Dienstes eine sehr hohe Anzahl von Fehlernachrichten erzeugt, die nur schwer zu erfassen und hinsichtlich der zugrunde liegenden Fehlerursache bzw. Angriffsursache zu analysieren.

Bei heutigen bekannten Verwaltungswerkzeugen für die Behebung von Störungen in dem Kommunikationsnetz erfolgt keine systematische Überwachung des Telekommunikationsnetzes hinsichtlich sicherheitsmäßig auffälliger oder bedenklicher Aktivitäten von Komponenten in dem Telekommunikationsnetz, die auf einer Gesamtsicht auf das Kommunikationsnetz beruht.

Weiterhin existieren auf der Ebene der OSI-Schicht 2 und der OSI-Schicht 3 des **O**pen **S**ystem **I**nterconnection-Referenzmodells (OSI-Referenzmodell) der **I**nternational **O**rganization for **S**tandardization (ISO) auf unterschiedliche Kommunikationsprotokolle eingeschränkte Möglichkeiten zur Erkennung der Topologie, der Struktur von miteinander gekoppelten Kommunikationsgeräten in einem Telekommunikationsnetz.

Diese grundsätzlich auf vorhandene Strukturen beschränkte Erkennung erlaubt jedoch keine Rückschlüsse auf tatsächliche Beziehungen zwischen den einzelnen Geräten in dem Telekommunikationsnetz im Sinne des aktiven Verhaltens der einzelnen Geräte und/oder der verwendeten Dienste und deren Nutzung.

Diese Beziehungen lassen sich gemäß den bekannten Kommunikationsprotokollen auch nicht automatisch in ausreichend großem Maße extrahieren.

Auf der Ebene höherer OSI-Schichten, beispielsweise der Darstellungsschicht (OSI-Schicht 6) oder der Anwendungsschicht (OSI-Schicht 7) des OSI-Referenzmodells, auf der üblicherweise die Anwendungsprogramme implementiert sind, werden gemäß dem Stand der Technik die einzelnen Abhängigkeitsbeziehungen zwischen den Kommunikationsgeräten bzw. den verwendeten

Diensten manuell eingegeben und in unterschiedlichen Sprachen und Darstellungsformen entsprechend dem verwendeten Protokollformat formuliert.

Diese Vorgehensweise eignet sich jedoch aufgrund der Ermangelung einer einheitlichen allgemeinen Beschreibung der Struktur des Telekommunikationsnetzes nicht für den Einsatz in einem realen größeren Telekommunikationsnetz.

Insbesondere bei einer erhöhten Anzahl von Geräten und/oder Diensten, die über das Telekommunikationsnetz miteinander kommunizieren, ist eine manuelle Überwachung der einzelnen Geräte bzw. Dienste in dem Telekommunikationsnetz nicht mehr praktikabel bzw. überhaupt nicht mehr möglich.

Somit liegt der Erfindung das Problem zugrunde, kommunikationsfähige Geräte und/oder Dienste, die über ein Telekommunikationsnetz miteinander kommunizieren, automatisiert und auf verglichen mit dem Stand der Technik einfachere Weise zu überwachen.

Das Problem wird durch das Verfahren und die Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes sowie durch das Verfahren zum rechnergestützten Trainieren eines statistischen Schätzers zum Überwachen eines Telekommunikationsnetzes, die Computerlesbaren Speichermedien sowie die Computerprogramm-Elemente mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

Bei einem Verfahren zum rechnergestützten Überwachen eines Telekommunikationsnetzes, welches eine Vielzahl von kommunikationsfähigen Geräten und/oder Diensten aufweist, werden von zumindest einem Teil der Geräte bzw. Dienste Kommunikationsparameter ermittelt, die die Aktivität des jeweiligen Gerätes bzw. Dienstes beschreiben.

Unter Aktivität eines Geräts bzw. eines Dienstes ist in diesem Zusammenhang beispielsweise die Rechnerauslastung eines Prozessors, den das Gerät aufweist bzw. der den Dienst ausführt, oder auch die Kommunikationsaktivität mit anderen Geräten bzw. Diensten über das Kommunikationsnetz, das heißt der Grad des Sendens und des Empfangens von Daten, vorzugsweise von digitalen Daten, die in Datenpakete gruppiert sind, zu verstehen.

Die ermittelten Kommunikationsparameter werden mittels eines mit Trainingsdaten trainierten statistischen Schätzers mit einem aus ermittelten Abhängigkeiten zwischen den Geräten ermittelten Normal-Abhängigkeitsbereich verglichen und aus dem Vergleich wird bestimmt, ob das Kommunikationsverhalten eines oder mehrerer Geräte bzw. Dienste, die an das Telekommunikationsnetz angeschlossen sind, sich von deren Normalverhalten, das heißt von deren ungestörten Verhalten gemäß einem vorgegebenen Kriterium, beispielsweise um einen vorgegebenen Toleranzbereich, unterscheidet.

Anders ausgedrückt bedeutet dies, dass ermittelt wird, ob ein oder mehrere Geräte bzw. Dienste sich in ihrem Verhalten hinsichtlich eines vorgegebenen Vergleichskriteriums gegenüber dem zuvor ermittelten Normal-Abhängigkeitsbereich in vorgegebener Weise unterscheiden oder nicht.

Bei einem Verfahren zum rechnergestützten Trainieren eines rechnergestützten Schätzers, welcher zum Überwachen eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten und/oder Diensten eingesetzt wird, werden von zumindest einem Teil der Geräte und/oder Dienste Kommunikationsparameter ermittelt, die die Aktivität des jeweiligen Gerätes bzw. Dienstes beschreiben.

Aus den Aktivitätsdaten, im Weiteren auch als Aktivitätsparameter bezeichnet, also den Kommunikationsparametern bzw. der Rechnerauslastung der Geräte bzw. Dienste werden mögliche Ab-

hängigkeiten zwischen den Geräten bzw. Diensten in Bezug auf deren Kommunikation miteinander ermittelt und aus den ermittelten Abhängigkeiten wird ein Normal-Abhängigkeitsbereich ermittelt, mit dem Abhängigkeiten zwischen den Geräten bzw. Diensten in einem Zustand im Wesentlichen ohne Störung der Geräte bzw. Dienste und ohne Angriffsversuche von einem Gerät oder durch ein Gerät bzw. von einem Dienst oder durch einen Dienst, beschrieben werden.

Mit dem üblichen Verhalten der Geräte bzw. Dienste, das heißt mit dem Normal-Abhängigkeitsbereich wird der statistische Schätzer trainiert.

Eine Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten weist einen Prozessor auf, mit dem die oben beschriebenen Verfahrensschritte sowohl des Verfahrens zur Überwachung als auch des Verfahrens zum Trainieren des statistischen Schätzers zum Überwachen der kommunikationsfähigen Geräte, die mit dem Telekommunikationsnetz gekoppelt sind, durchgeführt werden können.

Weiterhin sind in Computerlesbaren Speichermedien Computerprogramme zum rechnergestützten Überwachen eines Telekommunikationsnetzes sowie zum Trainieren eines statistischen Schätzers zum Überwachen eines Telekommunikationsnetzes gespeichert, die, wenn sie von einem Prozessor ausgeführt werden, die oben beschriebenen Verfahrensschritte der entsprechenden Verfahren aufweisen.

Ferner weisen Computerprogramm-Elemente zum rechnergestützten Überwachen des Telekommunikationsnetzes sowie zum rechnergestützten Trainieren eines statistischen Schätzers zum Überwachen eines Telekommunikationsnetzes die oben beschriebenen Verfahrensschritte der entsprechenden Verfahren auf, wenn sie von einem Prozessor ausgeführt werden.

Durch die Erfindung wird es erstmals möglich, auf Ebene der Anwendungsschicht oder der Darstellungsschicht des OSI-Referenzmodells eine Vielzahl unterschiedlichster Geräte bzw. Dienste hinsichtlich derer Ausfälle bzw. bezüglich möglichen Angriffsversuchen zu überwachen, obwohl die einzelnen mit dem Telekommunikationsnetz gekoppelten Geräte bzw. Dienste sehr inhomogen, das heißt mittels unterschiedlichster Protokolle auf unterschiedlichen Schichten des OSI-Referenzmodells arbeiten.

Ein weiterer erheblicher Vorteil der Erfindung ist darin zu sehen, dass auch automatisiert die Abhängigkeiten der einzelnen Geräte untereinander, gemäß einer Ausgestaltung der Erfindung sogar paarweise, berücksichtigt werden können und somit in die automatisierte Überwachung mit einbezogen werden können.

Auf diese Weise wird die Überwachung von Geräten und Diensten sehr effizient automatisch durchführbar und somit kostengünstig.

Ferner wird die automatisierte Überwachung insbesondere durch eine auf statistischen Methoden basierende Analyse großer anfallender Datenmengen hinsichtlich einer möglichen Fehlerursache bzw. eines möglichen Angriffsversuchs erheblich verbessert und effizienter gestaltet.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Zumindest ein Teil der Geräte kann als kommunikationsfähiges Endgerät ausgestaltet sein.

Die Ermittlung der Aktivitätsparameter kann in einem vorgegebenen Zeitintervall, welches für alle oder zumindest einen Teil der Geräte in dem Kommunikationsnetz gleich oder unterschiedlich sein kann, erfolgen.

Auf diese Weise wird auch eine zeitliche Veränderung des Verhaltens der einzelnen Geräte bzw. Dienste insbesondere hinsichtlich der Kommunikationsaktivität der einzelnen Geräte bzw. Dienste möglich, wodurch die Genauigkeit der Überwachung weiter verbessert wird.

Gemäß einer weiteren Ausgestaltung der Erfindung ist es vorgesehen, dass die Ermittlung der Aktivitätsparameter von dem jeweiligen Gerät selbst durchgeführt wird und die ermittelten Aktivitätsparameter werden an eine zentrale Verwaltungseinheit übertragen, in der die weiteren Verfahrensschritte durchgeführt werden.

So ist es beispielsweise gemäß einer Weiterbildung der Erfindung vorgesehen, dass unter Einsatz eines Netzmanagementprotokolls, beispielsweise mittels des Simple Network Management Protokolls (SNMP) in einer Management Information Base (MIB) die ermittelten Aktivitätsparameter gespeichert werden und entsprechend gemäß dem SNMP-Protokoll von der Verwaltungseinheit die Aktivitätsparameter aus der MIB abgefragt werden und an die Verwaltungseinheit übertragen werden.

Gemäß einer alternativen Ausgestaltung der Erfindung ist es vorgesehen, dass die Ermittlung der Aktivitätsparameter von einer Aktivitätsparameter-Ermittlungseinheit außerhalb des jeweiligen Geräts durchgeführt wird, das heißt beispielsweise von einer Vermittlungseinheit, die unterschiedliche Kommunikationsparameter an einer äußeren Schnittstelle des jeweiligen Geräts ermittelt.

Für den Fall, dass die Aktivitätsparameter beispielsweise die Anzahl gesendeter oder von dem jeweiligen Gerät empfangener Datenpakete ist, wird als Kommunikationsparameter die Anzahl der unmittelbar mit dem jeweiligen Gerät gekoppelten Vermittlungseinheit ermittelten Datenpakete verwendet.

Die Abhängigkeiten können kommunikationsbedingte Abhängigkeiten zwischen den Geräten bzw. Diensten sein, die gemäß einer Ausgestaltung der Erfindung eine Richtungsabhängigkeit hinsichtlich der Kommunikationsrichtung zwischen den einzelnen Geräten bzw. Diensten aufweisen können.

Unter einer Richtungsabhängigkeit ist beispielsweise zu verstehen, dass unterschieden wird, ob ein Gerät bzw. ein Dienst eine Nachricht oder ein Datenpaket sendet oder empfängt.

Durch diese Weiterbildung wird die Überwachung der Geräte bzw. Dienste in dem Telekommunikationsnetz weiter in ihrer Genauigkeit verbessert, da ein zusätzlicher Parameter, nämlich die Richtungsabhängigkeitsangabe, berücksichtigt wird.

Die unmittelbar von aus den Kommunikationsdaten ermittelten Daten können einer Vorverarbeitung unterschiedlicher Art, beispielsweise einer Filterung oder einer statistischen Voranalyse unterzogen werden und aus den vorverarbeiteten Daten können die Kommunikationsparameter ermittelt werden, die zur Überwachung unmittelbar verwendet werden.

Durch die Vorverarbeitung wird eine weitere Effizienzerhöhung im Rahmen der Überwachung erreicht.

Es können insbesondere für die kommunikationsbedingten Abhängigkeiten zwischen den Geräten jeweils paarweise Abhängigkeiten für jeweils ein Gerätepaar bzw. ein Dienstepaar, das heißt jeweils für alle möglichen Kombinationen zweier in dem Telekommunikationsnetz miteinander gekoppelten Geräte bzw. Dienste die Aktivitätsparameter ermittelt werden.

Auf diese Weise wird eine paarweise Betrachtung der Abhängigkeiten ermöglicht und somit die Ermittlung möglicher Fehlerursachen weiter vereinfacht.

Gemäß einer weiteren Ausgestaltung der Erfindung ist es vorgesehen, dass die ermittelten Aktivitätsparameter der Gerätepaare bzw. Dienstepaare in Form einer Matrix gespeichert werden und dass der Normal-Abhängigkeitsbereich aus der Struktur der ermittelten Matrix bestimmt wird.

Somit wird eine strukturelle Abhängigkeit zwischen den einzelnen Zeilen bzw. Spalten der Matrix, in denen die jeweiligen Abhängigkeiten angegeben sind, das heißt beispielsweise die Kommunikation zwischen den einzelnen Geräten bzw. Dienste, die jeweils eine Zeile bzw. eine Spalte der Matrix repräsentieren, ermittelt.

Die Struktur der gebildeten Matrix wird mittels des statistischen Schätzers "erlernt" und es erfolgt im Rahmen der Anwendungsphase im Rahmen der Überwachung der jeweiligen Geräte eine im Wesentlichen graphische und somit sehr einfache strukturelle Überwachung mittels des statistischen Schätzers.

Die Aktivitätsparameter können beispielsweise eine der folgenden Parameter sein:

- eine Anzahl der von dem jeweiligen Gerät bzw. Dienst gesendete Datenpakete oder von dem jeweiligen Gerät bzw. Dienst empfangene Datenpakete,
- die Prozessorauslastung des jeweiligen Geräts,
- die Anzahl vorgegebener Systemfunktionsaufrufe beispielsweise von Betriebssystemfunktionen des Betriebssystems, welches das jeweilige kommunikationsfähige Gerät verwendet bzw. das den jeweiligen Dienst durchführt,
- die Existenz vorgegebener Prozesse bzw. vorgegebener Computerprogramme während des Zeitraums, während dessen die Kommunikationsparameter für das jeweilige Gerät bzw. den jeweiligen Dient ermittelt werden.

Als statistischer Schätzer kann beispielsweise ein grundsätzlich beliebiges neuronales Modell, das heißt ein neuronales Netz oder auch ein Neuro-Fuzzy-Modell verwendet werden, wel-

ches mit bekannten Trainingsmethoden und eventuell zusätzlich mit sogenannten Pruning-Verfahren trainiert wird.

Für den Fall, dass sich mindestens ein Gerät bzw. Dienst in dem Telekommunikationsnetz in vorgegebenem Maße von dem Kriterium hinsichtlich des Normal-Abhängigkeitsbereichs in seinem Verhalten unterscheidet, wird ein Alarmsignal generiert und einem Benutzer des Überwachungssystems dargestellt, beispielsweise als Audiosignal oder auch auf einem Bildschirm als graphisches Alarmsignal.

Auf diese Weise wird automatisiert dem Verwalter eines Telekommunikationsnetzes eine Warnung zugänglich gemacht, dass sich mit einer entsprechend großer Wahrscheinlichkeit ein Gerät bzw. Dienst in dem Telekommunikationsnetz befindet, welches bzw. welcher gestört ist oder sogar ausgefallen ist oder welches bzw. welcher einen Angriffsversuch auf ein anderes Gerät bzw. auf einen anderen Dienst startet oder welches bzw. welcher selbst mit einem unbefugten Zugriffsversuch angegriffen wird.

In diesem Zusammenhang ist anzumerken, dass das Training des statistischen Schätzers sowohl Offline als auch zusätzlich oder alternativ Online, das heißt während der Anwendungsphase, während der schon eine Überwachung des Telekommunikationsnetzes stattfindet, erfolgen kann.

Gemäß einer alternativen Ausgestaltung ist es ferner vorgesehen, den statistischen Schätzer als ein oder mehrere miteinander gekoppelter gepulster Neuronen auszugestalten.

Somit kann die Erfindung sowohl zum Ermitteln einer Störung eines Geräts bzw. Dienst in dem Telekommunikationsnetz und/oder zum Ermitteln eines unbefugten Zugriffsversuchs auf ein oder von einem Gerät Dienst in dem Telekommunikationsnetz eingesetzt werden.

Die oben dargestellten Ausgestaltungen der Erfindung betreffen sowohl die Verfahren, die Vorrichtungen als auch die Computerlesbaren Speichermedien und die Computerprogramm-Elemente.

Die Erfindung kann sowohl mittels einer speziellen elektronischen Schaltung, d.h. in Hardware, als auch mittels eines Computerprogramms, d.h. in Software, implementiert sein.

Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im Weiteren näher erläutert.

Es zeigen

Figur 1 eine Skizze eines Telekommunikationsnetzes gemäß einem Ausführungsbeispiel der Erfindung;

Figur 2 eine Skizze der Struktur eines neuronalen Modells, mit dem die Abhängigkeit der Aktivitätsparameter zwischen zwei kommunikationsfähigen Geräten gemäß einem Ausführungsbeispiel der Erfindung repräsentiert wird;

Figur 3 eine Skizze, anhand der ein Mustervergleich zweier Matrizen dargestellt ist, in denen die Abhängigkeiten der Aktivitätsparameter zwischen den jeweiligen Geräten in dem Telekommunikationsnetz dargestellt sind;

Figur 4 ein Ablaufdiagramm, in dem die einzelnen Verfahrensschritte des Verfahrens gemäß einem Ausführungsbeispiel der Erfindung dargestellt sind.

Fig.1 zeigt ein Telekommunikationsnetz 100 mit einer Vielzahl kommunikationsfähiger Geräte wie Personal Computer 101, 102, 103, 104, Terminals 105, 106, 107, Laptops 108, 109, einer Workstation 110, einem Firewall-Computer 111 sowie einem Zentralcomputer 112, die über das Telekommunikationsnetz 100

miteinander sowie mit einem zentralen Verwaltungsrechner 113 gekoppelt sind.

Die Terminals 105, 106, 107 sind über Leitungen 114 mit dem Zentralrechner 112 sowie über ein lokales Netzwerk 115 mit dem zentralen Verwaltungsrechner 113 gekoppelt.

Ferner sind über den Firewall-Computer 111 die Personal Computer 101, 102, 103, 104, die Laptops 108, 109 sowie die Workstation 110 mittels Kommunikationsverbindungen 116 unter Verwendung des Internet-Protokolls mit dem zentralen Verwaltungsrechner 113 gekoppelt.

Mittels des zentralen Verwaltungsrechners 113 als zentrale Verwaltungseinheit werden die mittels des Telekommunikationsnetzes 113 miteinander gekoppelten kommunikationsfähigen Geräte gemäß dem im Weiteren beschriebenen Verfahren überwacht.

In einem ersten Schritt werden, wie im Weiteren im Detail erläutert, die einzelnen Kommunikationsparameter für die jeweiligen kommunikationsfähigen Geräte ermittelt (Schritt 401), wie in dem Ablaufdiagramm 400 in **Fig.4** dargestellt ist.

Gemäß dem Ausführungsbeispiel werden als Aktivitätsparameter folgende, die Aktivität der jeweiligen Geräte in dem Telekommunikationsnetz 100 beschreibende Größen hinsichtlich des Datenverkehrs zwischen jeweils einem Gerätepaar, das heißt jeweils zweier Geräte innerhalb des Telekommunikationsnetzes 100 ermittelt.

Es werden in einer Trainingsphase jeweils nur Daten für den Verkehr zwischen zwei Geräten ausgewählt und es werden verschiedene vorgegebene Anwendungsprogramme, beispielsweise typische Anwendungsprogramme wie ein Web-Server-Programm oder eine X-Anwendung gestartet und ausgeführt, wobei alle restlichen Geräte in dem Telekommunikationsnetz 100 ausgeschaltet sind oder die Daten für den Verkehr zwischen den zwei spezi-

fischen Geräten beispielsweise anhand der IP-Adressen (Internet Protocol-Adressen) isoliert werden können.

Anschaulich wird somit jeweils nur die aufgrund der ausgeführten Applikationen bzw. der ausgeführten Dienste unmittelbar erzeugte Kommunikation bzw. Auslastung des jeweiligen Gerätes und eventuell ein Datenverkehr, das heißt eine Kommunikation zwischen den beiden ausgewählten Geräten, bei einem digitalen Datenaustauschmittel beschrieben durch die Anzahl gesendeter bzw. empfangener Datenpakete gemäß dem UDP-Protokoll innerhalb eines vorgegebenen Zeitintervalls.

Es werden für jede Anwendung und für jedes Gerätepaar, das heißt für alle möglichen Kombinationen von Anwendung/Geräten in dem Telekommunikationsnetz 100 jeweils auf die oben beschriebene Weise die folgenden Kommunikationsparameter ermittelt auf der Basis einer Anzahl einer in jeweils einem 5-Sekunden-Intervall ermittelten Anzahl von dem jeweiligen Gerät empfangenen, das heißt bei dem jeweiligen Gerät ankommenden Datenpakete werden unter Einsatz unterschiedlicher Vortransformationen, das heißt einer entsprechenden Vorverarbeitung der Kommunikationsparameter unterzogenen Datenpakete, ermittelt:

- Die Anzahl der Datenpakete, jedoch gemittelt über mehrere 5-Sekunden-Intervalle und mittels einer Normierungsfunktion optional normiert;

- ein Korrelationswert der ausgetauschten Datenpakete zwischen den Geräten über 30 Sekunden, das heißt über sechs 5-Sekunden-Intervalle bzw. 100 Sekunden, das heißt über zwanzig 5-Sekunden-Intervalle.

  Der ermittelte Korrelationswert Corr(x, y, n) wird gemäß folgender Vorschrift ermittelt:

$$Corr(x, y, n) = \frac{\sum_{i=0}^{n-1} (x_{t-i} - \bar{x}) \cdot (y_{t-i} - \bar{y})}{\sqrt{\left(\sum_{i=0}^{n-1} (x_{t-i} - \bar{x})^2\right) \cdot \left(\sum_{i=0}^{n-1} (y_{t-i} - \bar{y})^2\right)}}, \quad (1)$$

wobei mit

- n die Anzahl berücksichtigter Werte, bei 30 Sekunden somit n = 6 und bei 100 Sekunden n = 20, bezeichnet wird,
- x die jeweilige Anzahl empfangener Datenpakete des ersten Geräts zu dem entsprechend berücksichtigten Zeitpunkt bezeichnet wird,
- y die jeweilige Anzahl empfangener Datenpakete des zweiten Geräts zu dem entsprechend berücksichtigten Zeitpunkt bezeichnet wird,
- $\bar{x}$, $\bar{y}$ jeweils der gleitende Mittelwert der letzten n-Werte (t − n + 1) bis zu dem Zeitpunkt t des ersten bzw. des zweiten Geräts bezeichnet wird.

- Der Betrag der Differenz der jeweils ankommenden Pakete des ersten Geräts des Gerätepaars und des zweiten Geräts des Gerätepaars, das jeweils betrachtet wird;

- Der Minimum-Wert der während jeweils eines 5-Sekunden-Intervalls ermittelten Anzahl der bei einem der beiden Geräte des Gerätepaars ankommenden Datenpakete.

Unter Verwendung der ermittelten Kommunikationsparameter, die für eine Vielzahl von Trainingsintervallen ermittelt werden, wird jeweils für ein Trainingsintervall ein Trainingsdatum ermittelt und dem in **Fig.2** dargestellten neuronalen Netz 200 zu dessen Training zugeführt.

Das neuronale Netz 200 weist eine Eingangsschicht 201 mit zehn Eingangsneuronen auf, die über jeweils eine Eins-zu-Eins-Verbindung als Identitäts-Abbildung mit einer Vorverar-

beitungsschicht 202, die ebenfalls zehn Neuronen aufweist, gekoppelt sind.

Es ist jeweils ein Neuron der Vorverarbeitungsschicht 202 mit einem Neuron der Eingangsschicht 201 gekoppelt.

Weiterhin ist eine, beispielsweise in [1] beschriebene lokale Modellierungsschicht 203 mit den Neuronen der Vorverarbeitungsschicht 202 gekoppelt.

Eine versteckte Schicht 204 mit einer grundsätzlich beliebigen Anzahl von Neuronen ist sowohl mit den Neuronen der Vorverarbeitungsschicht 202 als auch mit den Neuronen der lokalen Modellierungsschicht 203 gekoppelt.

Weiterhin ist die versteckte Schicht 204 über die Ausgänge ihrer Neuronen mit Neuronen einer Ausgangsschicht 205 gekoppelt, die Ausgabewerte 206 erzeugen.

Das Training der neuronalen Anordnung 200 erfolgt auf übliche Weise, beispielsweise mittels eines Backpropagation-Trainingsverfahrens unter Einsatz eines Pruning-Verfahrens wie beispielsweise in [1] beschrieben.

Es ist jeweils ein neuronales Netz 200 der in **Fig.2** dargestellten Struktur für jedes Gerätepaar der in dem Telekommunikationsnetz 100 enthaltenen Geräte vorgesehen und das neuronale Netz 200 wird für dieses Gerätepaar entsprechend auf die oben beschriebene Weise trainiert.

Mittels des neuronalen Netzes 200 ist es somit möglich, sowohl lokale Zusammenhänge als auch globale Zusammenhänge des Kommunikationsverhaltens des jeweiligen Gerätepaars zu modellieren.

Sind m Geräte über das Telekommunikationsnetz 100 miteinander gekoppelt, so sind $\frac{(m-1)^2}{2}$ Kombinationen Daten zu erheben und dem neuronalen Netz 200 zum Training zuzuführen.

Das gemäß dem oben beschriebenen Verfahren trainierte neuronale Netz 200 wird kopiert und liefert somit für jedes Gerätepaar bei Anlegen der Eingangsdaten eine Ausgabe. Natürlich können auch mehrere, verschiedene, spezialisierte neuronale Netze verwendet werden. Somit kann das oben beschriebene Verfahren für jedes Gerätepaar der Geräte in dem Telekommunikationsnetz durchgeführt werden, wie in Schritt 402 des Ablaufdiagramms 400 dargestellt.

Alternativ kann zur Erhöhung der Genauigkeit für verschiedene Kombinationen von Gerätetypen jeweils ein eigenes neuronales Netz trainiert werden.

Ergebnis des Schritts 402 ist dann eine Anzahl von $\frac{(m-1)^2}{2}$ gleicher oder verschiedener neuronaler Netze 200 (bei m verschiedenen Gerätetypen), die auf die oben beschriebene Weise trainiert worden sind.

Aufgrund des Ausgabeverhaltens dieser neuronalen Netze 200 für unterschiedliche Trainingsdaten wird eine Ausgabestruktur ermittelt und beispielsweise in Form einer Matrix 300, wie sie in **Fig.3** dargestellt ist, gespeichert.

Fig.3 zeigt in einer Matrix 300 jeweils in einer Spalte 301 bzw. einer Zeile 302 der Matrix 300, welche jeweils ein Gerät in dem Telekommunikationsnetz 100 repräsentiert, in jeweils einem Feld die dem Grad der Abhängigkeit des Netzverkehrs, das heißt der ankommenden Datenpakete aufgrund der trainierten neuronalen Netze 200, die jeweils die Abhängigkeit des Datenverkehrs zwischen den einzelnen Gerätepaaren angeben, an.

Die Felder können sowohl über eine graphische Repräsentation als auch über einen vorgebbaren Zahlenwert, der den Grad der Abhängigkeit des Datenverkehrs repräsentiert, beschrieben werden.

Anschaulich ist in **Fig.3** durch unterschiedliche Schattierung bzw. Schraffierung jeweils ein unterschiedlicher Grad der Abhängigkeit der unterschiedlichen Netzaktivitäten der jeweiligen Gerätepaare eingetragen.

Es ergibt sich somit eine graphische Abhängigkeitsstruktur, die im Weiteren als Trainingskarte 303 bezeichnet wird.

Ein zweites neuronales Modell, gemäß dem Ausführungsbeispiel ein Neuro-Fuzzy-Modell, wird anschließend eingesetzt, um abhängig von den Trainingsdaten aus der Trainingsphase die ermittelte Trainingskarte 303, die die Abhängigkeiten aus der Trainingsphase beschreibt, mittels bekannter Trainingsverfahren zu erlernen.

Während der Anwendungsphase werden die entsprechenden Aktivitätsparameter kontinuierlich ermittelt und es wird eine Anwendungskarte 304 auf die oben beschriebene gleiche Weise ermittelt, wie die Trainingskarte 303 während des Trainingsverfahrens ermittelt worden ist.

Selbstverständlich wird in der Anwendungsphase nicht jedes Gerät individuell jeweils mit einem weiteren Gerät als Gerätepaar untersucht, sondern es werden jeweils für die entsprechenden Zeitintervalle die ankommenden Datenpakete bei dem jeweiligen Gerät ermittelt. Dies erfolgt jeweils unter Verwendung der jeweiligen Adressenangaben in den Datenpaketen die der Sender bzw. Empfänger des Datenpakets ermitteln kann, wodurch die entsprechenden Korrelationen zwischen den einzelnen Gerätepaaren in der Anwendungsphase ermittelt werden.

Das sich in der Anwendungsphase ergebende Bild als Anwendungskarte 304 wird in einem weiteren Schritt (Schritt 404) mittels des Neuro-Fuzzy-Modells mit der Trainingskarte 303 verglichen.

Unterscheidet sich die Anwendungskarte 304 gemäß einem vorgegebenen Ähnlichkeitskriterium stärker als ein vorgegebener Schwellenwert, der einen Toleranzbereich aufweisen kann, so wird ein Alarmsignal generiert (Schritt 405), mit dem angezeigt wird, dass eine auffällige Netzaktivität bei mindestens einem Gerät bzw. Dienst in dem Telekommunikationsnetz 100 ermittelt worden ist aufgrund einer unterschiedlichen Kartenstruktur der Anwendungskarte 304 verglichen mit der Trainingskarte 303.

Somit kann entweder aufgrund dieses Vergleichsergebnisses, welches zu dem Alarmsignal führt, auf einen Ausfall eines oder mehrerer Geräte in dem Telekommunikationsnetz 100 geschlossen werden oder darauf, dass von einem Gerät aus ein Angriffsversuch in ein weiteres Gerät in dem Telekommunikationsnetz 100 gestartet wird, oder dass auf einem Gerät ein unbefugter Zugriffsversuch, das heißt ein Angriffsversuch, unternommen wird.

Wird keine auffällige Netzaktivität in dem Prüfungsschritt 404 ermittelt, so wird das Überwachungsverfahren in einem wiederholten Ermitteln einer Anwendungskarte 304 in einer erneuten Anwendungsphase (Schritt 403) durchgeführt.

Das Verfahren wird solange durchgeführt, bis es entweder durch den Benutzer des Netzverwaltungssystems, das heißt den Benutzer der zentralen Verwaltungseinheit 113 beendet wird, oder bis das Alarmsignal generiert worden ist (Schritt 405).

In diesem Dokument ist folgende Veröffentlichung zitiert:

[1] G.B. Orr, Neural Networks: tricks of the trade, K.-R. Müller (ed.), Berlin, Springer, ISBN 3-540-65311-2, (Lecture notes in computer science, Vol. 1524), 1998

Patentansprüche

1. Verfahren zum rechnergestützten Überwachen eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten,

- bei dem von zumindest einem Teil der Geräte und/oder von Diensten Aktivitätsparameter ermittelt werden, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- bei dem die ermittelten Aktivitätsparameter mittels eines mit Trainingsdaten trainierten statistischen Schätzers mit einem aus ermittelten Abhängigkeiten zwischen den Geräten ermittelten Normal-Abhängigkeitsbereich verglichen werden, und
- bei dem aus dem Vergleich bestimmt wird, ob das Kommunikationsverhalten zumindest eines Geräts und/oder zumindest eines Dienstes in dem Telekommunikationsnetz sich von dem Normal-Abhängigkeitsbereich gemäß einem vorgegebenen Kriterium unterscheidet.

2. Verfahren zum rechnergestützten Trainieren eines statistischen Schätzers zum Verwalten eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten,

- bei dem von zumindest einem Teil der Geräte und/oder von Diensten Kommunikationsparameter ermittelt werden, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- bei dem aus den Kommunikationsparametern der Geräte und/oder Dienste mögliche Abhängigkeiten zwischen den Geräten und/oder Diensten ermittelt werden,
- bei dem aus den ermittelten Abhängigkeiten ein Normal-Abhängigkeitsbereich ermittelt wird, mit dem Abhängigkeiten zwischen den Geräten und/oder Diensten in einem Zustand im wesentlichen ohne Störungen beschrieben wird, mit dem der statische Schätzer trainiert wird.

3. Verfahren nach Anspruch 1 oder 2,

bei dem zumindest ein Teil der Geräte als kommunikationsfähiges Endgerät ausgestaltet ist.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die Ermittlung der Aktivitätsparameter in einem vorgegebenen Zeitintervall erfolgt,

5. Verfahren nach einem der Ansprüche 1 bis 4,

- bei dem die Ermittlung der Aktivitätsparameter von dem jeweiligen Gerät durchgeführt wird, und
- bei dem die ermittelten Aktivitätsparameter an eine Verwaltungseinheit übertragen wird, in der die weiteren Verfahrensschritte durchgeführt werden.

6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem die Ermittlung der Aktivitätsparameter von einer Aktivitätsparameter-Ermittlungseinheit außerhalb des jeweiligen Geräts durchgeführt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6,
bei dem als Abhängigkeiten kommunikationsbedingte Abhängigkeiten zwischen den Geräten und/oder Diensten ermittelt werden.

8. Verfahren nach einem der Ansprüche 1 bis 7,
bei dem mögliche Richtungsabhängigkeiten hinsichtlich der Kommunikationsrichtungen zwischen den Geräten und/oder Diensten ermittelt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8,

- bei dem Daten von den Geräten und/oder Diensten ermittelt werden, und
- bei dem aus den Daten die Aktivitätsparameter ermittelt werden.

10. Verfahren nach einem der Ansprüche 1 bis 9,

bei dem für alle möglichen Gerätepaare und/oder Dienstepaaren jeweils zweier Geräte und/oder Dienste die Aktivitätsparameter ermittelt werden,

11. Verfahren nach Anspruch 10,

- bei dem die ermittelten Aktivitätsparameter der Gerätepaare in Form einer Matrix gespeichert werden, und
- bei dem der Normal-Abhängigkeitsbereich aus der Struktur der Matrix ermittelt wird.

12. Verfahren nach einem der Ansprüche 1 bis 11,
bei dem als Aktivitätsparameter zumindest einer der folgenden Parameter ermittelt werden:

- von dem jeweiligen Gerät und/oder Dienst gesendete Datenpakete oder von dem jeweiligen Gerät und/oder Dienst empfangene Datenpakete ermittelt werden,
- die Prozessorauslastung des jeweiligen Geräts ermittelt werden,
- die Anzahl vorgegebener Systemfunktionsaufrufe,
- die Existenz vorgegebener Prozesse bzw. vorgegebener Computerprogramme.

13. Verfahren nach einem der Ansprüche 1 bis 12,
bei dem als statistischer Schätzer ein Neuro-Fuzzy-Modell verwendet wird.

14. Verfahren nach einem der Ansprüche 1 bis 13,
bei dem für den Fall, dass sich mindestens ein Gerät in dem Telekommunikationsnetz von dem Normal-Abhängigkeitsbereich gemäß dem vorgegebenen Kriterium unterscheidet, ein Alarmsignal generiert wird.

15. Verfahren nach einem der Ansprüche 1 bis 14,
eingesetzt zum Ermitteln einer Störung eines Geräts in dem Telekommunikationsnetz und/oder zum Ermitteln eines unbefugten Zugriffsversuchs auf ein oder von einem Gerät in dem Telekommunikationsnetz.

16. Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten,
mit einem Prozessor, der derart eingerichtet ist, dass folgende Schritte durchführbar sind:

- von zumindest einem Teil der Geräte und/oder von Diensten werden Aktivitätsparameter ermittelt, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- die ermittelten Aktivitätsparameter werden mittels eines mit Trainingsdaten trainierten statistischen Schätzers mit einem aus ermittelten Abhängigkeiten zwischen den Geräten ermittelten Normal-Abhängigkeitsbereich verglichen, und
- aus dem Vergleich wird bestimmt, ob das Kommunikationsverhalten zumindest eines Geräts und/oder zumindest eines Dienstes in dem Telekommunikationsnetz sich von dem Normal-Abhängigkeitsbereich gemäß einem vorgegebenen Kriterium unterscheidet.

17. Computerlesbares Speichermedium, in dem ein Computerprogramm zum rechnergestützten Überwachen eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten gespeichert ist, das, wenn es von einem Prozessor ausgeführt wird, folgende Verfahrensschritte aufweist:

- von zumindest einem Teil der Geräte und/oder von Diensten werden Aktivitätsparameter ermittelt, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- die ermittelten Aktivitätsparameter werden mittels eines mit Trainingsdaten trainierten statistischen Schätzers mit einem aus ermittelten Abhängigkeiten zwischen den Geräten ermittelten Normal-Abhängigkeitsbereich verglichen, und
- aus dem Vergleich wird bestimmt, ob das Kommunikationsverhalten zumindest eines Geräts und/oder zumindest eines Dienstes in dem Telekommunikationsnetz sich von dem

Normal-Abhängigkeitsbereich gemäß einem vorgegebenen Kriterium unterscheidet.

18. Computerprogramm-Element zum rechnergestützten Überwachen eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten, das, wenn es von einem Prozessor ausgeführt wird, folgende Verfahrensschritte aufweist:

- von zumindest einem Teil der Geräte und/oder von Diensten werden Aktivitätsparameter ermittelt, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- die ermittelten Aktivitätsparameter werden mittels eines mit Trainingsdaten trainierten statistischen Schätzers mit einem aus ermittelten Abhängigkeiten zwischen den Geräten ermittelten Normal-Abhängigkeitsbereich verglichen, und
- aus dem Vergleich wird bestimmt, ob das Kommunikationsverhalten zumindest eines Geräts und/oder zumindest eines Dienstes in dem Telekommunikationsnetz sich von dem Normal-Abhängigkeitsbereich gemäß einem vorgegebenen Kriterium unterscheidet.

19. Computerlesbares Speichermedium, in dem ein Computerprogramm zum rechnergestützten Trainieren eines statistischen Schätzers zum Verwalten eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten gespeichert ist, das, wenn es von einem Prozessor ausgeführt wird, folgende Verfahrensschritte aufweist:

- von zumindest einem Teil der Geräte und/oder von Diensten werden Aktivitätsparameter ermittelt, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- aus den Aktivitätsparameter der Geräte und/oder Dienste werden mögliche Abhängigkeiten zwischen den Geräten und/oder Diensten ermittelt,
- aus den ermittelten Abhängigkeiten wird ein Normal-Abhängigkeitsbereich ermittelt, mit dem Abhängigkeiten

zwischen den Geräten und/oder Diensten in einem Zustand im wesentlichen ohne Störungen beschrieben wird, mit dem der statische Schätzer trainiert wird.

20. Computerprogramm-Element zum rechnergestützten Trainieren eines statistischen Schätzers zum Verwalten eines Telekommunikationsnetzes mit einer Vielzahl von kommunikationsfähigen Geräten, das, wenn es von einem Prozessor ausgeführt wird, folgende Verfahrensschritte aufweist:

- von zumindest einem Teil der Geräte und/oder von Diensten werden Aktivitätsparameter ermittelt, die die Aktivität des jeweiligen Geräts und/oder des jeweiligen Dienstes beschreiben,
- aus den Aktivitätsparameter der Geräte und/oder Dienste werden mögliche Abhängigkeiten zwischen den Geräten und/oder Diensten ermittelt,
- aus den ermittelten Abhängigkeiten wird ein Normal-Abhängigkeitsbereich ermittelt, mit dem Abhängigkeiten zwischen den Geräten und/oder Diensten in einem Zustand im wesentlichen ohne Störungen beschrieben wird, mit dem der statische Schätzer trainiert wird.

Zusammenfassung

Verfahren und Vorrichtung zum rechnergestützten Überwachen eines Telekommunikationsnetzes, Verfahren zum rechnergestützten Trainieren eines statistischen Schätzers, Computerlesbare Speichermedien und Computerprogramm-Elemente

Es werden zumindest von einem Teil der Geräte und/oder Dienste Aktivitätsparameter ermittelt, die die Aktivität des jeweiligen Geräts beschreiben. Die ermittelten Kommunikationsparameter werden mittels eines trainierten statistischen Schätzers mit einem aus ermittelten Abhängigkeiten zwischen den Geräten ermittelten Normal-Abhängigkeitsbereich verglichen und es wird bestimmt, ob das Kommunikationsverhalten der Geräte einem vorgegebenen Kriterium genügen.

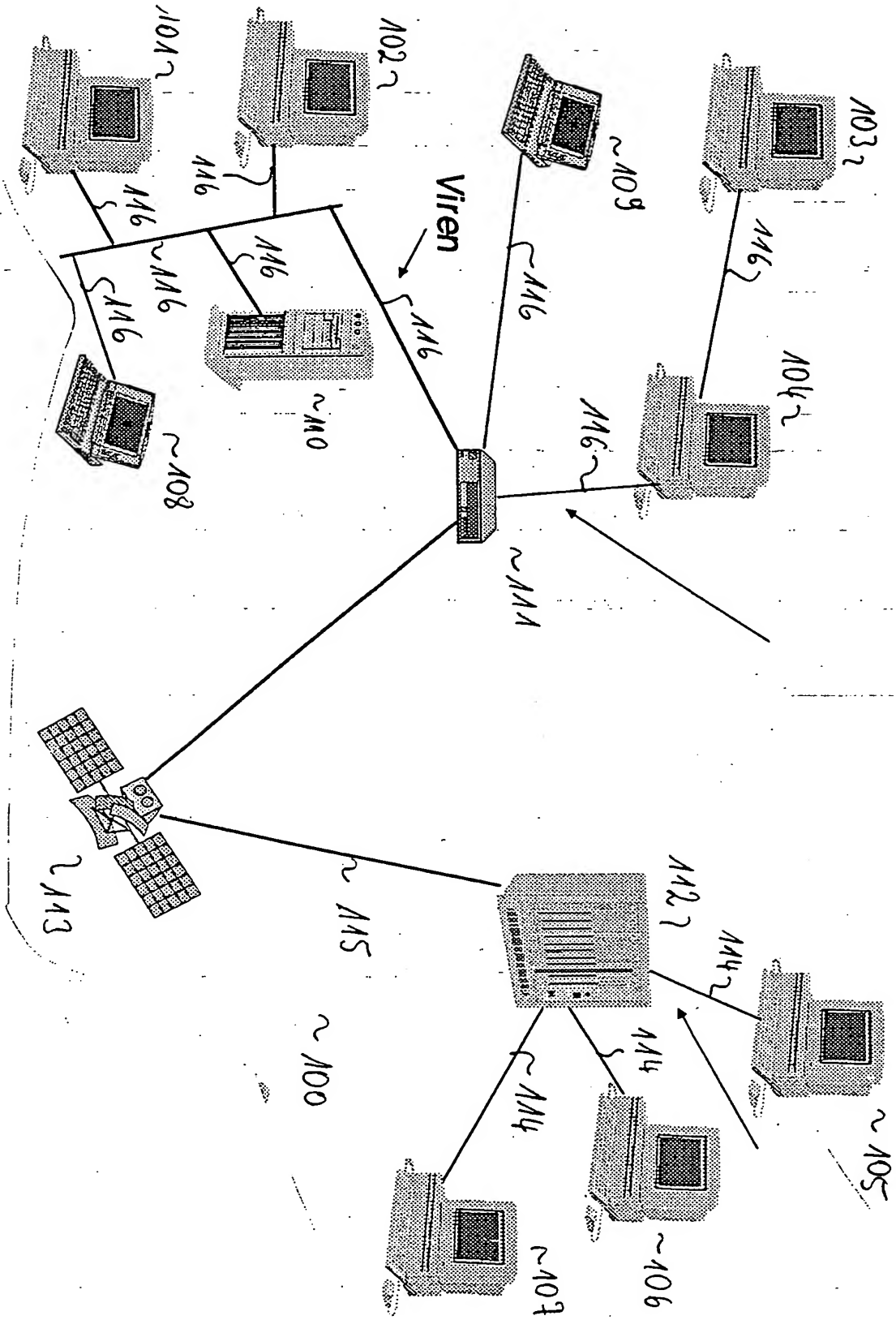
Figur 4

49E 8209

Loog P00426

E. DOLTER

FIG 1



99E 8209

2004P00426

E. DOLTER

FIG 2

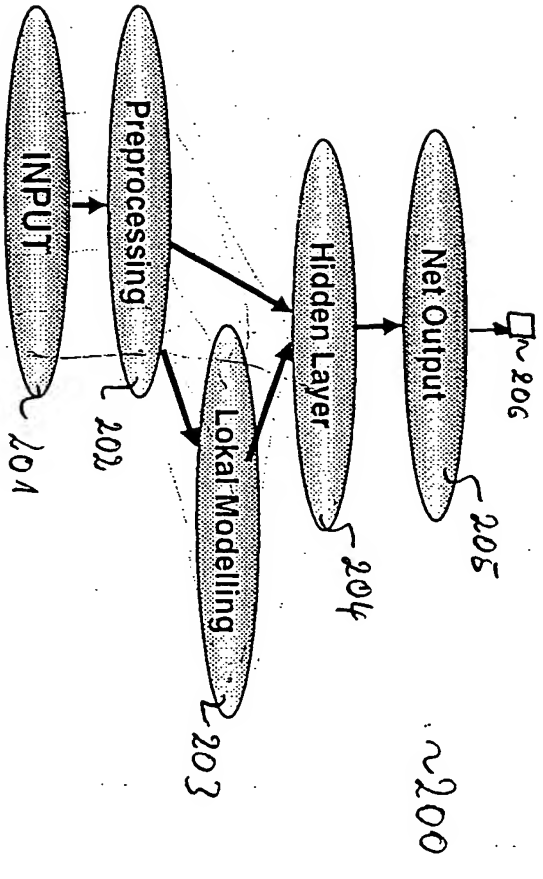


FIG3

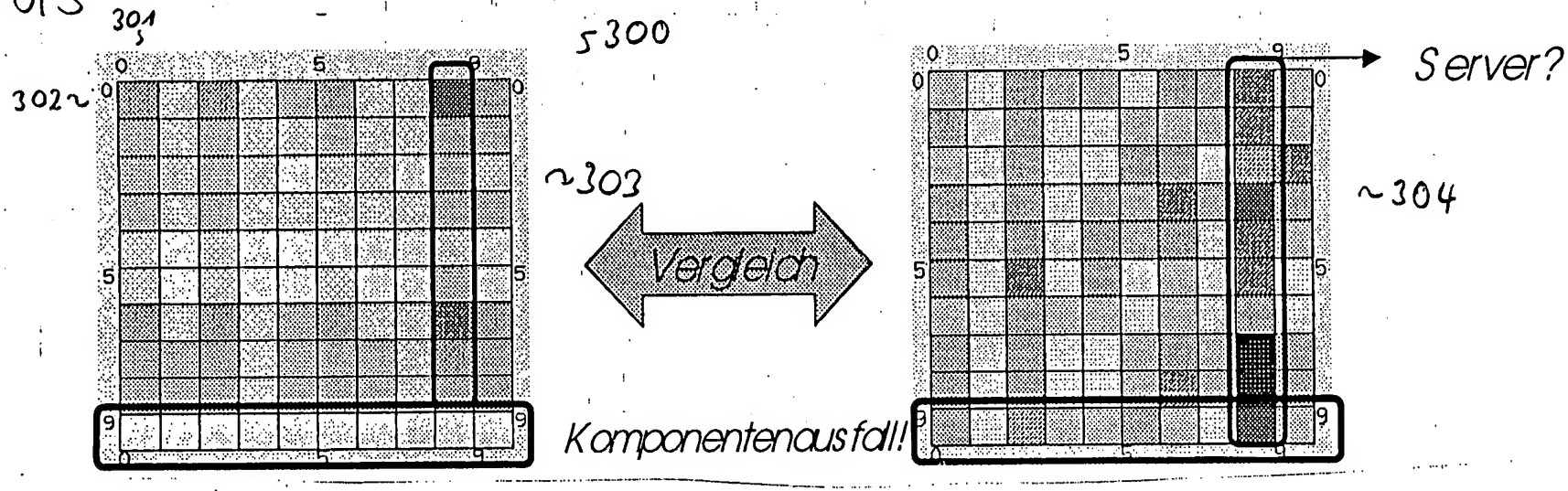


FIG 4